Deep Science Publishing
https://doi.org/10.70593/978-81-984306-5-6_1

Chapter 1

# Introduction to hybrid cloud paradigms: Bridging public and private clouds

Ravi Kumar Vankayalapati

*Cloud AI ML Engineer, Equinix, Dallas, USA.*
*ravikumar.vankayalapti.research@gmail.com*

## Abstract

The hybrid cloud paradigm represents a transformative approach to modern IT infrastructure, seamlessly integrating the scalability and flexibility of public clouds with the security and control of private clouds. This model enables organizations to optimize resource utilization, enhance agility, and address complex business demands by bridging disparate cloud environments. By leveraging hybrid cloud strategies, enterprises can deploy workloads dynamically across on-premises and cloud-based platforms, ensuring cost efficiency, data compliance, and operational resilience. This abstract explores the key principles, architectural frameworks, and technological advancements driving hybrid cloud adoption. It also highlights use cases across industries, the challenges of interoperability and management, and emerging trends in hybrid cloud solutions, offering insights into how businesses can achieve digital transformation through effective hybrid cloud implementations.

## Keywords

Hybrid Cloud, Public Cloud, Private Cloud, Cloud Computing, IT Infrastructure, Digital Transformation, Cloud Integration, Scalability, Data Compliance, Operational Resilience, Cloud Workloads, Cloud Management, Interoperability, Cloud Security, Cloud Architecture, Enterprise Cloud Strategy, Cloud Optimization, Cloud Adoption Trends.

## 1.1. Introduction

Cloud computing transforms the way information technology (IT) is consumed and managed, promising improved cost efficiencies, accelerated innovation, faster time-to-market, and the ability to scale applications on demand. There is a major shift towards the cloud computing model and that the benefits may be substantial. However, legal/contractual, economic, service quality, interoperability, security and privacy issues still pose significant challenges. A common understanding of cloud computing is that it represents a large pool of computing resources that can be easily and flexibly accessed and that is in some sense elastic i.e., users can increase or decrease the amount of pooled resources that they use and pay according to their amount of usage (Danda, 2022). Cloud computing refers to a class of systems in which tasks are assigned to a combination of connections, software services and computing devices such as large servers with numerous processors and data storage media, and code executed on virtual machines. It leverages the network of large data centers where servers can operate independently at scale and bulk data is stored encrypted on scale-out storage systems and replicated for fault tolerance on geographically distributed sites.

For an application to be classed as cloud computing it must be accessible via a convenient and standardized mechanism such as a service as well as being remotely hosted. It is a computing model that enables ubiquitous access to shared pools of configurable system resources and higher-level services that can be rapidly provisioned with minimal management effort often over a network and collaboratively used by multiple tenants. Some sources define it as storage and virtual machines in data centers with high utilization, effective allocation policies, large-scale solutions available on the internet (Syed, 2022). The telescoping of services running an application in a wide area network can be seen as a hardcore interpretation of this definition, but more generally it is utilized as an inside-out perspective. These four delivery models are attractive to any federal, state, or local agency for delivering and consuming services on different types of clouds. The agencies may employ one model or a combination of different models for efficient and optimized delivery of applications and business services.

### 1.1.1 Definition and Key Concepts

Cloud computing has in the last years become mainstream in the IT world. However, as with other hot topics, there is a lot of confusion about what cloud computing really is and how it differs from traditional IT infrastructure technologies. Defining cloud computing is challenging and various definitions can be found in the literature, each highlighting different aspects of cloud computing (Nampalli, 2022). In this work, the most important terms will be explained, trying to provide more clarity about what constitutes a cloud service and what does not.

There is a relationship between the different cloud service models (PaaS, IaaS and SaaS) and deployment models (private, public, community, hybrid) and that, for instance, a storage service offered under an IaaS deployment model will differ significantly from another storage service offered under a PaaS deployment model. Finally, four of the most common mistakes regarding cloud computing made by its detractors are discussed, offering the reasons why these claims are not based in reality.

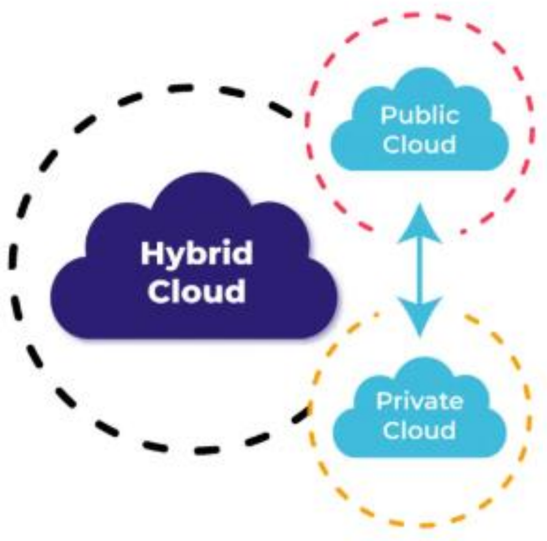


Fig 1.1: Public cloud, Private cloud and Hybrid cloud

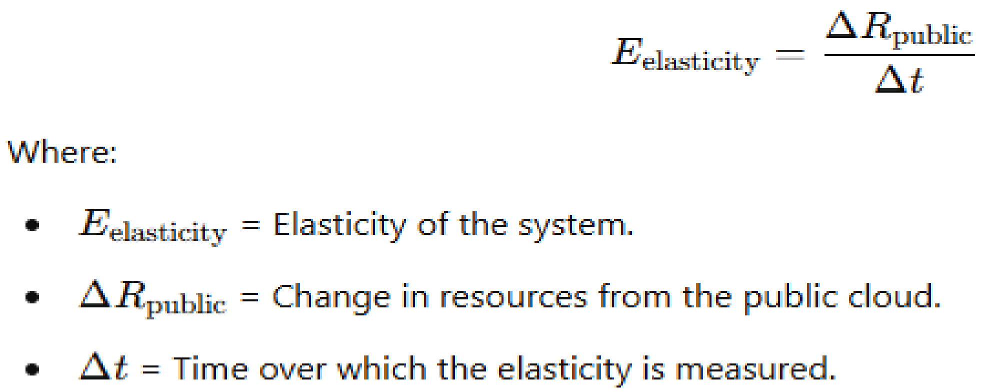
### 1.1.2 Evolution of Cloud Computing

The early 2000s saw a considerable flurry of interest in “utility computing”, which evolved from the telecommunication sector’s idea of delivering online services – providers would house large farms of servers (used as a “family” of services or “basket” of applications), which would be metered on a “use-as-you-go” basis (Danda, 2022). Although various attempts were made at developing such services and many systems used the utility moniker, there was little in the way of a coherent model for delivering services in such a way and it failed to break out from a niche market. It was not until the mid-2000s that a number of technological advances laid the necessary groundwork for the emergence of modern cloud computing. A surge in the development of cheap virtualization technologies, coupled with a proliferation of high-speed and robust broadband Internet and the rise of an increasingly large and mobile workforce armed with consumer electronic devices such as smartphones, spurred the initial wave of interest in the formerly maligned concept of thin-client computing. This combination of innovations saw the growth of online services, spurred on by providers such as Amazon and Google, who arguably kick-started the cloud industry in the 2010s. As a corollary, the need for IT business support, particularly in the agile development of Internet startups, resulted in an enhanced acceptance of external or outsourced IT infrastructure. This shifting business landscape also saw a parallel growth in other models of service delivery, the most relevant here being software as a service (SaaS) (Syed, 2022). This facilitated the activity of both established and new players, and here to a number of business models arose, such as collaboration solutions, CRM and e-commerce. Wedding these two technology vectors resulted in new forms of cloud services – essentially value-added services layered on top of the existing IaaS infrastructure. In sum, by the 2010s businesses were increasingly turning their backs on traditional on-premise solutions in favor of a new crop of public cloud offerings. The three main players in this shifting landscape, and central to the development of public cloud services, are Amazon, Google and Microsoft. Amazon's strategy has been to use their experience in virtualization and their infrastructure procurement (they own some of the largest server farms on the planet), to create a self-contained ecosystem that can provide the most efficient and low-cost services to customers. In contrast, Google has used its large-scale experience both in terms of operating a cloud and its search service, to develop a cloud offering that has the same infrastructure as Google's own internal services. Microsoft has strategically employed the resources of one of the largest software companies on Earth to expand its existing stable of business services (Office 365), and move its existing business customer base to the cloud.

## 1.2. Understanding Hybrid Clouds

The next generation of cloud computing is Hybrid Cloud. A hybrid cloud is an integrated cloud service utilizing qualitative and quantitative reasoning to apply solutions for a combination of public and private clouds that allows for data and applications portability across various cloud networks. In today's fast growing technology world, there is a continuum between private and public cloud services (Danda, 2020). Hybrid cloud is positioned as a natural consequence of technological maturation and evolution, since it encompasses services, solutions and products regarding or utilizing both public and private clouds.Specifically hybrid cloud is characterized by the capability to support the content of a given document or task with data retrieved from an integrated private or public cloud service. This document also investigates challenges, such as security or encryption, in assuring a safe and efficient connection between a private and public cloud service. An implemented structure of a document retrieval system on top of an integrated private and public cloud network is presented, as well as non-traditional implementations and applications involving the hybrid private and public cloud services are envisaged.

Equation 1: Elasticity Equation



$$E_{\text{elasticity}} = \frac{\Delta R_{\text{public}}}{\Delta t}$$

Where:

- $E_{\text{elasticity}}$ = Elasticity of the system.
- $\Delta R_{\text{public}}$ = Change in resources from the public cloud.
- $\Delta t$ = Time over which the elasticity is measured.

### 1.2.1 Definition and Characteristics

The definition of a hybrid cloud is a cloud containing two types of computing resources, where each type of resource has its own administrative domain (Subhash et al., 2022). A private cloud sets the administrator as the resource provider and only users authorized by the administrator are able to use the resources in the private cloud. The access to the private resources is secure but limited to the specific user group, and it is assumed that the resources in the private cloud are well protected as well. A public cloud opens its computing resources to the public and all users have equal access rights to the resources in the public cloud. The public cloud is scalable and ubiquitous but lacks secure connection to private resources. A hybrid cloud connects public cloud resources to private cloud resources and hence can make use of the convenience of public clouds while bringing the secure connection to the private resources. There is no restriction on the underlying technology in the implementation of the hybrid cloud. As long as a virtual private network can be established between the private cloud and the public cloud, the heterogeneous cloud systems, like a multi-vendor or multi-model cloud system can be connected to each other. A hybrid cloud system mainly contains the following characteristics. (a) The resources in the private cloud are assigned the administrator parameter specified by the parameter file, private, and vice versa to the resources in the public cloud. (b) The resources in the private cloud only have connections to the resources in the public cloud with a matching parameter file. (c) The parameters of the resources in the private cloud should match to the parameters of the job file from users trying to allocate the resource, and vice versa. (d) There is lack of connection among the computing resources of the private and the public clouds. Meanwhile a hybrid cloud has the (e) ability to scale resources dynamically based on job requests across two different cloud domains (Danda, 2021). The public clouds can provide unreserved and scalable computing resources which are free of burden to the cloud users who own their own limited resources. However, the problem is a public cloud is lacking in security connection to the private resources which are in charge of confidential results' generation or the large amount of raw data storage.

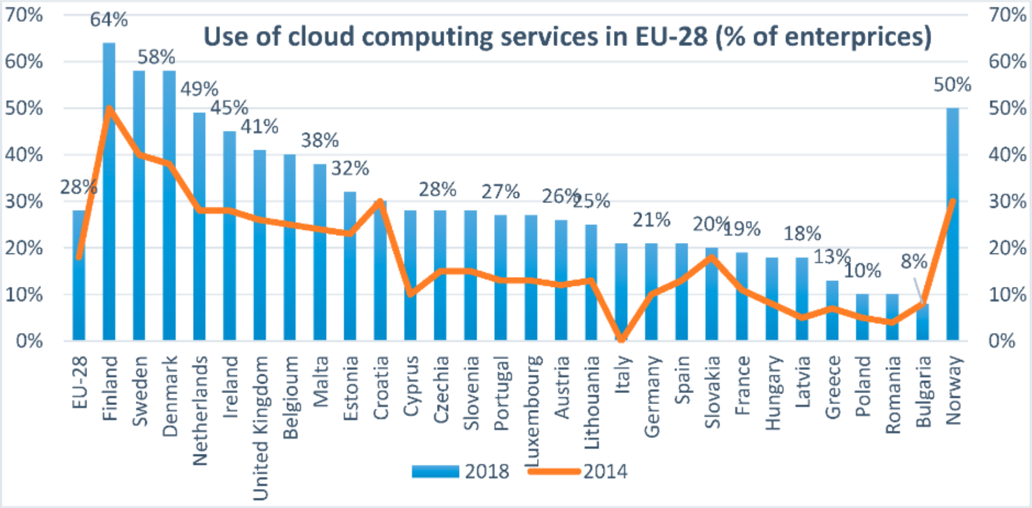


Fig: User Preferences on Cloud Computing and Open Innovation

### 1.2.2 Benefits and Challenges

Common industry practices and current research are also updated as a foundation for subsequent sections analyzing practical suggestions and architectural considerations. In addressing today's technology trends for this case, the focus area is primarily on public and private clouds, but it is recognized that there are other models of clouds and data centers. Recent days' emerging trends of IT environments are rapidly evolving into cloud computing paradigms (Vankayalapati et al., 2023). These new trends open up new business opportunities and challenges as well. Brief analyses are provided of public and private cloud paradigms with regard to their common adaptation aspects, benefits, and challenges. Concentrating on security, typical architectural models and frameworks are further introduced for designing (or extending) cloud based IT environments. With different goals, many other researchers can also consider these intros as a criterion or comparative work for more sophisticated security system configurations and model implementations. Offering network wide cloud services is a possibility for telecommunications carriers, and security services can protect information systems from external risks.

## 1.3. Architectural Design of Hybrid Clouds

Scalability is a chief advantage of public cloud infrastructure. The ideal public cloud infrastructure behaves like a large utility with virtually limitless compute and storage resources available on demand. In practice, the challenge is to create a balanced system that can allocate resources as needed for vastly different kinds of applications, workloads, and user bases. This will typically involve a hierarchy of resource types, each with a unique interface to describe requirements and a well-defined policy for allocation. One well-known example of this is, which allocates virtual machines with a stated number of processing cores, quantity of memory, and software images. It is also platform "agnostic," meaning clients can access it with a web service API from, and other languages. Another approach is to create an application-level overlay that brokers services among a federation of private and public clouds. Energy consumption and network congestion are monitored by an FCAPS-compliant device, which triggers application-level rules to redeploy VMs on the best facility. Each VSC is equipped with a VM-agent to ensure the creation, liveness, and connectivity of the VMs. On top of this is a light-weight, service-oriented, decentralized network, which tracks current load and VM capacity. Aggregating the above techniques results in an architecture in which a truly dynamic and evolvable network of services can be provisioned across hybrid Peers and cloud environments.

### 1.3.1 Public Cloud Infrastructure

Public cloud infrastructure is the fundamental building block of hybrid cloud models that bridge disparate public and private clouds. A public cloud consists of a massive infrastructure on a massive scale, as made available by commercial public cloud service providers, and it is per definition public. This means that there is a large number of users sharing the same resource pools (Ramanakar, 2022). Such public resources can be accessed over standard network connectivity and are typically offered on a pay per use basis. The resources are scalable, and usage can rapidly scale up or down, allowing users to quickly scale out capabilities. Another important aspect of public resources is that they are elastic, i.e., resources can be allocated or de-allocated on demand. Such public cloud resources are often referred to as on-demand resources, as they can be activated or expanded quickly, on demand.

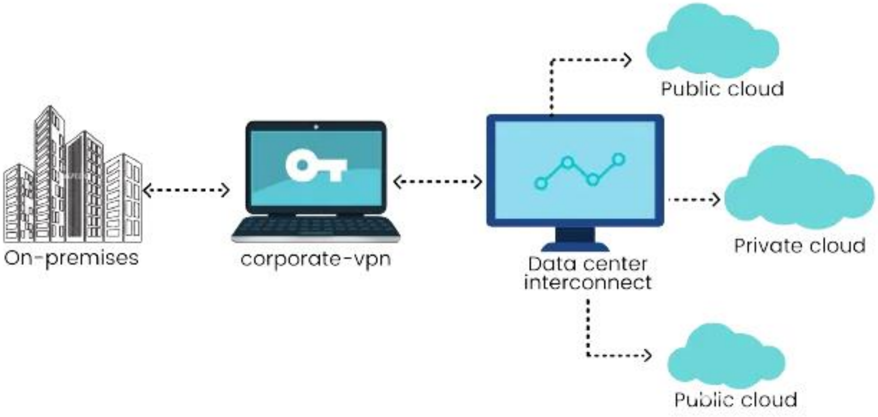


Fig 1.2: Hybrid Cloud Architectures

To effectively use public cloud resources, it is crucial to understand how these resources operate. The underlying compute resources are distributed, virtualized, and shared by a large number of tenants. As such there can be significant performance implications for certain usage and deployment scenarios, which are often not well understood by the commercial user. An in depth overview of how the resources are structured, service agreements which are typically in place, cost implications, and performance metrics which are often non-trivial is beyond the scope of this text, but will be addressed in upcoming detail. How this sharing model of public cloud resources impacts best use practices and common usage scenarios, will however be highlighted. Often the public resources are abstracted, and made available as different services or virtualization technologies, hiding the underlying detailed mechanics and tenant architecture. Thus it is important for the cloud user to understand in more detail how the operational mechanics of public resources work. Stripped down to its core, the major IaaS providers offer access to virtual computers and storage though web-interfaces, and a set of APIs.

### 1.3.2 Private Cloud Infrastructure

Private clouds can be implemented completely within an organization’s own datacenter or data centers while being built, managed, updated, and maintained by trained personnel.

In addition, a private cloud can exist on dedicated on- or offsite data centers hosted by a private cloud service provider that is also managed and maintained by trained personnel. A fully private cloud can also be implemented using a small number of robust data centers that are solely used by several related or partner organizations. The main advantage of a private cloud is having complete control over the cloud infrastructure, data, and applications which are being used and stored inside the private cloud. Besides, an organization's own internally managed firewall and trusted personnel increases the data and application security inside the private cloud. Therefore, private cloud can be seen as an extension of existing IT infrastructure with cloud advantages including scalability, agility and self-service. Virtualization and therefore servers can be used on private clouds for flexibility on resource allocation. Automation tools can also be utilized and can be developed to enable increasing/decreasing resources on demand which is also seen in a public cloud. It is possible to have a large amount of resources dedicated to a service even if the service is fluctuating. Generally, cost considerations include depreciation, maintenance, electricity, building heat cooling and operation of custom solutions for cloud automation. Choosing smaller servers can increase costs for collocation. Advantages of complete control should be purchased with the cost. Some of the challenges are the same challenges with public clouds such as ensuring availability, backups, redundancy, failover, monitoring, planning and following capacity usage. But some issues with public clouds are absent with private clouds such as compliance with laws and standards, improving safety and data security, and gaining trust. As safety improves, a hybrid cloud connection can be established. This explains why organizations can set up private clouds that meet their specific needs and then integrate them into a larger hybrid strategy at a later time. A discussion of these aspects is essential for understanding how private clouds fit within the broader cloud paradigm.

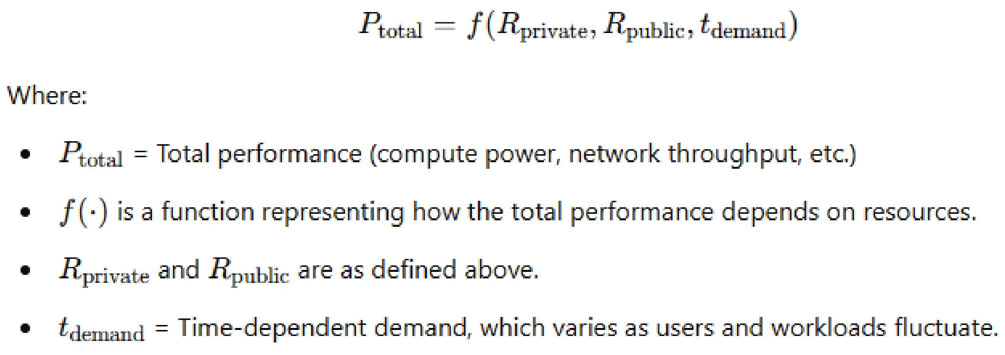
### 1.3.3 Integration and Interoperability

Three main paradigms that aim at merging public clouds with private/local IT infrastructures and their combination are tackled, providing a comprehensive account of the various efforts made in the domain. A hybrid cloud environment can highly benefit from seamless communication between the different cloud infrastructures it is composed of. Several guesstimates can be served over public clouds by blending them with a local platform. Virtualization in the data center. A local IT ecosystem is effectively collocated by virtual machines, which in turn can communicate with the hosted applications making use of a secured channel. However, combining public and private infrastructure under a coherent mechanism is a wholly different undertaking. Such environments are inherently incompatible, relying on distinct hardware, programming interfaces and security models.

Hence interoperability becomes a crucial issue for hybrid clouds. Public clouds are characterized by the ubiquity of services that are easily provisioned. The discern of them can be wrapped in Web APIs, making them straightforwardly available to applications running on servers across the globe. Data and application portability; ecosystem lock-in. A recent advancement in the cloud service distribution is the apparition of on-premises activities. This innovative model sanctions clients to subscribe to public cloud services embodied in their local private data center.

## 1.4. Use Cases and Applications of Hybrid Clouds

The variety and diversity of use cases and applications of hybrid clouds underscore their practicality and relevance in various sectors. Use case clouds offer a pre-constructed generic hybrid solution for a specific use case, so organizations can leverage hybrid clouds by adopting a pre-constructed solution more easily. Moreover, organizations are interested in using cloud resources based on their particular use case. Their custom application is executed and their data analytics platform is provisioned in hybrid clouds composed of private cloud execution resources and data analytics tools on a public cloud. In the Staging and On-demand provisioning phase, custom benchmarks are also being provisioned in the public cloud and executed on the data staging tool in the private cloud, as needed for public cloud execution. Custom benchmarks execute in the same manner as the stage-in tool in the public cloud, except that they download the dataset from the public cloud. Using the computation results of the WAN bandwidth benchmarks, the transformation goal is to decrease the dataset size (per Replica) by selecting the best dataset with the lowest size that contains, not more than 0.5% invalid data. Subsequently, the custom application is executed on the best size dataset to check if it is valid.



$$P_{\text{total}} = f(R_{\text{private}}, R_{\text{public}}, t_{\text{demand}})$$

Where:

- $P_{\text{total}}$ = Total performance (compute power, network throughput, etc.)
- $f(\cdot)$ is a function representing how the total performance depends on resources.
- $R_{\text{private}}$ and $R_{\text{public}}$ are as defined above.
- $t_{\text{demand}}$ = Time-dependent demand, which varies as users and workloads fluctuate.

Equation 2: Performance Scaling Equation

### 1.4.1 Hybrid Cloud in Enterprise Environments

The application was made to a custom cloud-based business intelligence and big data platform designed exclusively for enterprises consolidating multiple processes over millions of commodity items. Empowered by the hybrid cloud resources management, epoch-making reshaping has been done to the traditional control mechanism based on manual operations and the threshold setting is applied in processing, parallel, and inventory flows. An advanced inventory alert probability model is proposed by introducing the Poisson queue, and then to identify continuously the control points, a theoretical analysis is conducted by employing the state space and probability calculus. One of the most important issues for enterprises is how to maximize the competitive advantages and thus differentiate themselves from their competitors. Most important in the empirical results is a firm getting more value from hybrid cloud resources is the one capable of leveraging a different niche. For instance, a common practice consists in renting public cloud resources for non-critical scenarios and using private clouds to process sensitive information or care of critical processing. For a leading company, the private cloud is chosen for processing and thus key performance indicators (KPIs) go from a Web deployment with mining and learning purpose related to client-side interaction patterns of web servers, to encompass problem identification, root cause analysis, and impact prediction. Meanwhile, for the same client app server, monitoring KPIs are based on corresponding alert flows. In detail, the KPIs can be connected with client error. EXCEPTION, JDBCSQL Readable Data Cleck, server error EXCEPTION, and dp gbm error while turning privately aggregating alert frequencies from specific monitoring and processing rules, then public cloud resources are allotted in processing client-side I/O and corresponding gains are derived from mining alert patterns during market volatile days.

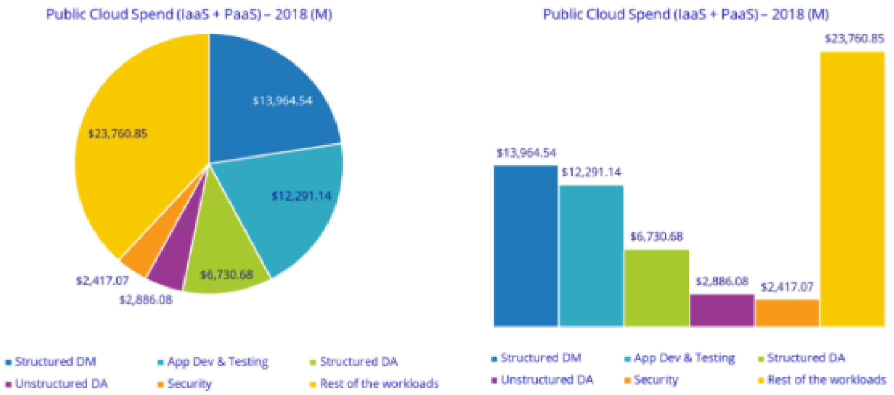


Fig: Public Cloud Services Spend - Segmented by Workloads

### 1.4.2 Hybrid Cloud for Data Storage and Processing

Realizing the advantages of the use of hybrid storage solutions, it is also worth considering the flexibility of an organization's infrastructure. Flexibility is realized by hybrid solutions without any additional expenses being incurred. The flexibility of using hybrid solutions seems to be essential because the workload generated by applications can change. One of the most popular storage solutions offered by cloud infrastructure providers is a service allowing the data to be stored. It is a scalable object storage service designed for massive and non-structured data. This service provides high durability of data and assures them to be available for download at any time for authorized clients. Moreover, the stored files are encrypted with strong encryption algorithms. Then, the stored file is split into smaller parts and added redundancy data. Once all the backup parts have been created using this strategy, data is sent to the cloud data storage. If the local storage is unavailable, the data can be recovered from the cloud storage. There is special software to ease this task, which is able to divide data into blocks and handle data transformation, so that data is protected before being sent to the data storage. To increase data security, it is possible to store the backup copy on other public storage in the cloud. In addition, there are data brokers that allow the copying of files between different companies. This can be the company's solution, ensuring the continuity of data storage using only one and the best cloud storage provider. Data brokers enable communication between stores in a different domain meaning offers the opportunity to exchange data between them. Overall, the hybrid approach shows high potential and perspective for infrastructure investment. At the same time storage costs are optimized, providing at the same time data availability and security with the use of both public and private storage solutions.

It is worth considering hybrid cloud solutions integrating public and private clouds where the company uses resources of multiple providers. Such integration is already possible, for example, mining and shipping out from different providers. Conversely, a private cloud resource might be obtained by a little IT business itself, while being, for example, an application provider. A hybrid approach can be advantageous. Regarding workflow intervals the data can be located in different cloud types. Data less important in terms of security and sensitivity can be hosted outside. Additionally, a public cloud provider can offer a service of storing, for example, backups. On the other hand, more critical data can be handled by a private one. Thanks to established standards, a standardized API is used for controlling cloud resources of multiple vendors. This API can also be used for a storage service and working based on used usage models. Mindfulness for planning a versatile solution can weaken or even counteract the technological advantages of the cloud. Security in terms of data governance and compliance on a regular basis comes to the fore in discussions with clients. Widely understood economic and public organizations have been required to treat data in line with regulations for years. Cloud-based solutions do not provide completely transparent tools, there may be a need to constantly exchange a standardized set of metadata - necessary, among other things for determining the location of the stored data itself. On the other hand, some activities related to data processing are required by law to take place only within the physical boundaries of a given country, hence the data cannot leave those boundaries in any form.

## 1.5. Security and Compliance Considerations in Hybrid Cloud Environments

Organisations are warming up to the cloud. While they recognise the benefits of cloud computing, such as cost reduction, scalability, and flexibility, some are hesitant to store certain sensitive data in the public cloud. The hybrid cloud is fast emerging as a preferred solution for such organisations. It allows them to store sensitive data in the private cloud and move less sensitive workloads like email to the public cloud. Implementing the hybrid cloud is relatively easy. Nonetheless, common vulnerabilities can emerge when organisations try to integrate a public cloud, often using third parties, with their in-house network. Interoperability between the two is one such concern. Each cloud usually has its own application interfaces. It is a challenge to get the application programming interfaces (API) to interact with each other so that workloads can share data. Another concern is the lack of encryption between the private and public cloud. A common tactic to bridge the two is to compress the workload data within the in-house network before moving them to the cloud. Last, adherence to regulatory frameworks and standards is seen as critical in addressing the above vulnerabilities.

Data residing in most countries need to comply with certain standards. For example, Singapore has the Personal Data Protection Act, under which all personal data must have appropriate protection and security in accordance with the Act. To guarantee this, any workloads being compressed and moved to the cloud should have data masked to avoid any personal information being shared. When using the hybrid cloud, it is essential to possess strong security measures. Workloads are compressed and sent to the public cloud. To decrypt that and retrieve the real data, they need to have VPN connections in place. This can be enhanced further by imposing IP and MAC filtering, so only certain legitimate IP and MAC are able to access the workload. For added protection, an intrusion prevention device can also be employed at the edge of the public cloud. Like any protection mechanism, it is important to continuously monitor during the data transfer and have robust incident response procedures in place. Hash files can be run periodically to ensure data integrity has not been compromised. Eye in the sky software can be deployed at the public cloud so that every packet going in and out can be scrutinised. Finally, countersurveillance devices such as covert pinhole cameras are recommended in the in-house network to constantly challenge any would-be attackers.

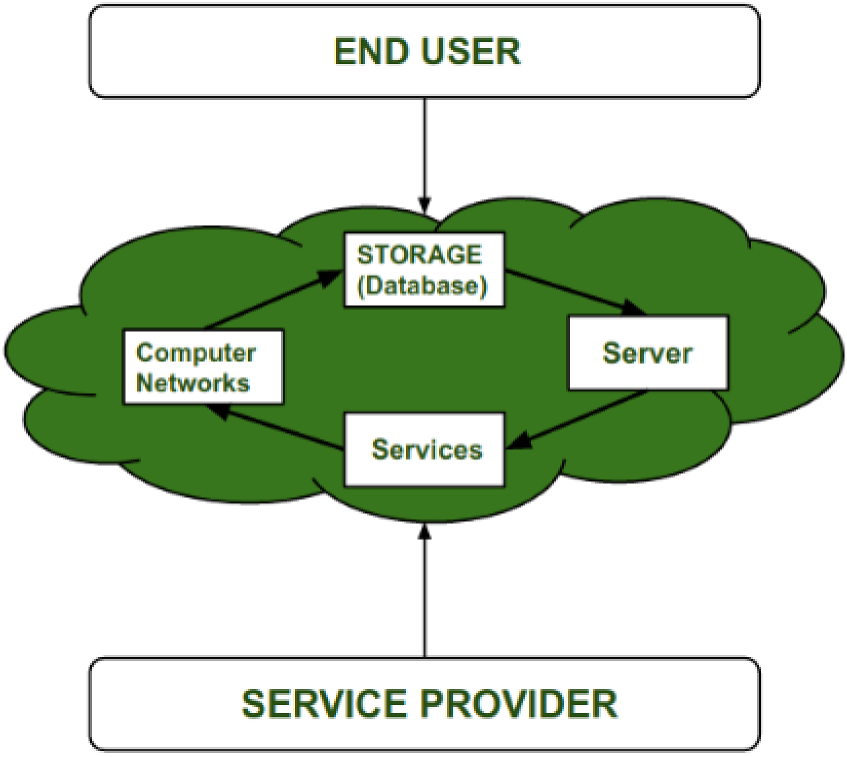


Fig 1.3: Security Issues in Cloud Computing

## 1.6. Conclusion

Cloud computing has revolutionized the storage, processing, and delivery of information since it was born in the late 1990s. However, cloud computing has several important issues, such as latency, costs, storage problems, security, privacy concerns, regulatory compliance, and bandwidth limits. To solve these issues, hybrid clouds come into play in today’s IT environment.

Hybrid clouds blend the characteristics of public and private clouds to leverage the benefits of both off-premises and on-premises resources for data and applications. The integration of private and public clouds to share data and applications and the use of encrypted communications will ensure privacy and security. It integrates public and private cloud resources and develops processed data and applications using both clouds.

The broadly flexible and common connectivity infrastructure will deliver reliable, safe, secure data exchange within the premises under cloud and external servers and resources. It bestows reliable, safe, exchanging big data and services from various clouds as computing resources.

These clouds aim to reduce the gap between public and private clouds, making it easier to develop hybrid clouds. The installation of virtual machines and physical hardware on servers will also ensure that all operating systems can deploy processed applications. Send usability of applications, telemedicine on the cloud will not have unserved messages and downtime that could be detrimental to patients. Moreover, patients can also get medical and health care services from long-distance hospitals and medical centers as well as general practitioners. Hybrid cloud computing provides flexibility, cost savings, and scalability. Thus, hybrid cloud solutions are very secure and maintain the private policy between the clouds, enabling public and processed clouds to exchange data, information, and resources.

### 1.6.1. Future trends

In the bid to optimize resources and reduce costs in infrastructure management, the reality of implementing public, private, and hybrid clouds is on the rise. The authors present a survey on the latest hybrid cloud paradigms, providing critical insights on bridging public and private clouds. In-depth reviews on state-of-the-art research contributions in hybrid cloud models, system architecture, and significant techniques are elaborated. Open issues and challenges in adapting hybrid clouds are also identified.

Emergence of hybrid cloud research can be related to the ever-growing explosive volume of users and data demands in cloud computing over recent years. The question of where and how to fulfill users' applications and services is challenged in physical or/and virtual infrastructural aspects. It is impractical for a single cloud service provider to have a global infrastructure that complements the range of capability, price, systematic, resilience, and regulatory. Research has been made in collaborative cloud federations that can share resources transparently across multiple physical data centers and cloud platforms. Also, many hybrid clouds have been introduced, maintaining valuable assets in private clouds, while harnessing public clouds for handling bursts. More recently, cloud-centric approach allows cloud users to extend their applications into hybrid clouds by horizontally federating multiple public-cloud providers.

## References

Danda, R. R. (2020). Predictive Modeling with AI and ML for Small Business Health Plans: Improving Employee Health Outcomes and Reducing Costs. In International Journal of Engineering and Computer Science (Vol. 9, Issue 12, pp. 25275–25288). Valley International. https://doi.org/10.18535/ijecs/v9i12.4572

Danda, R. R. (2021). Sustainability in Construction: Exploring the Development of Eco-Friendly Equipment. In Journal of Artificial Intelligence and Big Data (Vol. 1, Issue 1, pp. 100–110). Science Publications (SCIPUB). https://doi.org/10.31586/jaibd.2021.1153

Danda, R. R. (2022). Application of Neural Networks in Optimizing Health Outcomes in Medicare Advantage and Supplement Plans. Journal of Artificial Intelligence and Big Data, 2(1), 97–111. Retrieved from https://www.scipublications.com/journal/index.php/jaibd/article/view/1178

Danda, R. R. (2022). Deep Learning Approaches For Cost-Benefit Analysis Of Vision And Dental Coverage In Comprehensive Health Plans. Migration Letters, 19(6), 1103-1118.

Nampalli, R. C. R. (2022). Machine Learning Applications in Fleet Electrification: Optimizing Vehicle Maintenance and Energy Consumption. In Educational Administration: Theory and Practice. Green Publication. https://doi.org/10.53555/kuey.v28i4.8258

Ramanakar Reddy Danda. (2022). Telehealth In Medicare Plans: Leveraging AI For Improved Accessibility And Senior Care Quality. Migration Letters, 19(6), 1133–1143. Retrieved from https://migrationletters.com/index.php/ml/article/view/11446

Subhash Polineni, T. N., Pandugula, C., & Azith Teja Ganti, V. K. (2022). AI-Driven Automation in Monitoring Post-Operative Complications Across Health Systems. Global Journal of Medical Case Reports, 2(1), 1225. Retrieved from https://www.scipublications.com/journal/index.php/gjmcr/article/view/1225

Syed, S. (2022). Integrating Predictive Analytics In to Manufacturing Finance: A Case Study On Cost Control And Zero-Carbon Goals In Automotive Production. Migration Letters, 19(6), 1078-1090.

Syed, S. (2022). Towards Autonomous Analytics: The Evolution of Self-Service BI Platforms with Machine Learning Integration. In Journal of Artificial Intelligence and Big Data (Vol. 2, Issue 1, pp. 84–96). Science Publications (SCIPUB).https://doi.org/10.31586/jaibd.2022.1157

Vankayalapati, R. K., Sondinti, L. R., Kalisetty, S., & Valiki, S. (2023). Unifying Edge and Cloud Computing: A Framework for Distributed AI and Real-Time Processing. In Journal for ReAttach Therapy and Developmental Diversities. Green Publication. https://doi.org/10.53555/jrtdd.v6i9s(2).3348